Source : www.livemint.com Date : 2021-03-23

# INDIA MAY RAISE CHINESE HACK RISK AT GLOBAL FORUMS

Relevant for: International Relations | Topic: India - China

The move comes in the wake of repeated cyberattacks targeting India’s critical infra

India is looking to raise on the global stage the threat posed by Chinese hackers targeting its critical infrastructure such as power grids, according to two senior government officials aware of the development.

This is being discussed within the top levels of the government and comes against the backdrop of Red Echo, a hacker group affiliated with the Chinese government, repeatedly targeting the control rooms that manage India’s critical power grids. The massive campaign could have caused widespread blackouts. However, the Chinese hackers failed to break into the systems, and no data breach was detected, according to an earlier statement from power ministry.

The National Critical Information Infrastructure Protection Centre (NCIIPC), which oversees India’s cybersecurity operations in critical sectors, sounded an alert on 12 February about Red Echo targeting Regional Load Dispatch Centres (RLDCs) and State Load Dispatch Centres (SLDCs).

“We are thinking to formally state this because nothing in China is private in the strictest sense. There are various international committees on this, with cybersecurity being one of the important areas of cooperation. The idea is to take this up in different global forums," said one of the two officials mentioned above.

Queries emailed to the Prime Minister’s Office and the ministries of power, and electronics and information technology on 15 March were not answered till press time.

The armies of the two countries have disengaged at one of the friction points along their border in Ladakh even as they seek a mutually acceptable solution to the remaining issues of dispute.

“NCIIPC informed through a mail dated 12 February 2021 about the threat by Red Echo through a malware called Shadow Pad. It stated that: ‘Chinese state-sponsored threat actor group known as Red Echo is targeting Indian power sector’s Regional Load Dispatch Centres (RLDCs) along with State Load Dispatch Centres (SLDCs)’," according to a 1 March Union power ministry statement.

The NCIIPC warning was preceded by an alert from the Indian Computer Emergency Response Team (CERT-In) on 19 November 2020 that coordinates efforts on cybersecurity issues, on the threat of a malware called Shadow Pad at some control centres of Power System Operation Corp. Ltd (Posoco), which oversees India’s critical electricity load management functions.

“We may take this up at the appropriate forums. This is not the India of 1947 and we are not going to be cowed down. You are targeting the population by destabilizing the power system. If you switch off the power, the economy will grind to a halt," said the official quoted above.

“When the Mumbai outage was being investigated, it was found that several malwares were in the IT system of the SLDC," said a third person, not mentioned above, who also did not want to be named.

India is also improving its capability in dealing with sophisticated cyberattacks by state actors as power infrastructure remains their key target.

“We are working on hardening the grid," said a fourth person, not mentioned above, referring to India’s national power grid.

A report published in *The New York Times* linked last year’s grid failure in Mumbai to Chinese cyberattacks. The power outage in Mumbai disrupted emergency services and brokerages and halted local trains, considered the lifeline of India’s financial capital.

The *NYT* report cited US cybersecurity firm Recorded Future, which claimed the cyberattacks may have been linked to the military clash in Galwan Valley in June.

Although China refutes the allegation as “rumours and slander", India’s power sector reports at least 30 cyberattacks daily, *Mint* reported on 11 September 2019.

The ministry of road transport and highways on Sunday said that it has received an alert on targeted intrusion activities directed towards India’ transport sector.

**END**